Report No. DODIG-2012-080 April 24, 2012

Inspector General
United States Department of Defense

Improvements Are Needed to the Defense Finance and Accounting Service Information Assurance Vulnerability Management Program

Additional Copies

To obtain additional copies of this report, contact the Secondary Reports Distribution Unit at (703) 604-8937 (DSN 664-8937) or fax (571) 372-7469.

Suggestions for Audits

To suggest or request audits, contact the Office of the Deputy Inspector General for Auditing by phone (703) 604-9142 (DSN 664-9142), by fax (571) 372-7469, or by mail:

Department of Defense Office of Inspector General
Office of the Deputy Inspector General for Auditing
ATTN: Audit Suggestions/13F25-04
4800 Mark Center Drive
Alexandria, VA 22350-1500

Acronyms and Abbreviations

CIO	Chief Information Officer
CYBERCOM	U.S. Cyber Command
DFAS	Defense Finance and Accounting Service
IAVA	Information Assurance Vulnerability Alert
IAVM	Information Assurance Vulnerability Management
POA&M	Plan of Action and Milestones
VMS	Vulnerability Management System

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

April 24, 2012

MEMORANDUM FOR COMMANDER, U.S. STRATEGIC COMMAND
COMMANDER, U.S. CYBER COMMAND
DOD CHIEF INFORMATION OFFICER
DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE
DIRECTOR, JOINT STAFF

SUBJECT: Improvements Are Needed to the Defense Finance and Accounting Service Information Assurance Vulnerability Management Program (Report No. DODIG-2012-080)

~~(FOUO)~~ We are providing this report for your review and comment. The Defense Finance and Accounting Service Chief Information Officer did not properly remediate network vulnerabilities or report compliance. For example, 199 network assets with 507 vulnerabilities from August 2011 remained unpatched as of October 2011. If Defense Finance and Accounting Service does not address all vulnerabilities in a timely manner, its network and the DoD Global Information Grid are at risk of loss, misuse, or unauthorized access to sensitive information. We considered management comments on a draft of this report when preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. The Defense Finance and Accounting Service comments on Recommendations 1.c and 1.e were partially responsive. We request that the Defense Finance and Accounting Service Chief Information Officer provide additional comments by May 24, 2012.

Please provide comments that conform to the requirements of DoD Directive 7650.3. If possible, please send a portable document format (.pdf) file containing your comments to audros@dodig.mil. Copies of the management comments must contain the actual signature of the authorizing official for your organization. We are unable to accept the /Signed/ symbol in place of the actual signature. If you arrange to send classified comments electronically, you must send them over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 604-(b) (6) (DSN 664-(b) (6)

(b) (6)

Alice F. Carey
Assistant Inspector General
Readiness, Operations, and Support

Report No. DODIG-2012-080 (Project No. D2011-D000LB-0230.000) April 24, 2012

Results in Brief: Improvements Are Needed to the Defense Finance and Accounting Service Information Assurance Vulnerability Management Program

What We Did

Our objective was to determine whether the Defense Finance and Accounting Service (DFAS) implemented effective processes for managing and mitigating system vulnerabilities. This is the second of a series of audits.

What We Found

~~(FOUO)~~ DFAS did not always have effective processes to manage and mitigate system vulnerabilities. Specifically, the DFAS Chief Information Officer (CIO):

- did not remediate 507 of 1,007 vulnerabilities identified on the DFAS network as of October 2011;
- did not accurately report compliance for 42 of 51 active vulnerability alerts between September 2010 and August 2011; and
- could not support the number of affected assets, such as workstations and servers, reported for 28 of 52 sample vulnerability alerts.

~~(FOUO)~~ DFAS processes were not always effective because

- they permitted use of a 99-percent asset compliance threshold to mitigate vulnerabilities and did not mandate use of compliance reports and system administrators to report affected assets;
- DoD did not update vulnerability management guidance;
- the Vice Director, Joint Staff cancelled the vulnerability management manual; and
- U.S. Cyber Command did not specify the vulnerability alert requirements for patching vulnerabilities identified after the mitigation date.

~~(FOUO)~~ As a result, the risk of compromising sensitive DoD information on the DFAS network increased. In addition, inaccurate compliance reporting can reduce the effectiveness of U.S. Cyber Command oversight.

What We Recommend

~~(FOUO)~~ We recommend that the DFAS CIO:

- approve a plan of action and milestones for all affected network assets that are not patched by the mitigation date;
- report full compliance only when all affected network assets are patched; and
- use compliance reports and system administrators to identify affected assets;

We also recommend that the DFAS Deputy Director, Strategy and Support review actions of the DFAS CIO to determine if he acted within the scope of his authority to use a 99-percent asset compliance threshold.

Management Comments and Our Response

The management comments received were either responsive or partially responsive. We request that DFAS CIO provide additional comments on the final report by May 24, 2012. Please see the recommendations table on the back of this page.

Recommendations Table

Management	Recommendations Requiring Comment	No Additional Comments Required
Deputy Director, Strategy and Support, Defense Finance and Accounting Service		2
Chief Information Officer, Defense Finance and Accounting Service	1.c, 1.e	1.a, 1.b, 1.d

Please provide comments by May 24, 2012.

Table of Contents

Table of Contents (cont'd)

Introduction

Objective

This is the second in a series of audits on vulnerability management. Our objective was to determine whether the Defense Finance and Accounting Service (DFAS) implemented effective processes for managing and mitigating system vulnerabilities* in accordance with the DoD Information Assurance Vulnerability Management (IAVM) program. See Appendix A for a discussion of our scope and methodology and prior coverage. Finally, see Appendix C for the definitions of technical terms used in this report.

Background

DoD has a crucial responsibility to protect and defend its information and supporting information technology. For example, the loss, misuse of, or unauthorized access to sensitive DoD information could adversely affect the national interest, the conduct of Federal programs, or individual privacy. The Commander, U.S. Cyber Command (CYBERCOM), [1] testified before the House Committee on Armed Services in March 2011 and stated,

> [a]fter all, even the most astute malicious cyber actors-those who can break into almost any network that they really try to penetrate-are usually searching for targets of opportunity. They search for easy vulnerabilities in our systems security and then exploit them. I am very concerned by the ways in which neglect makes us vulnerable. The unapplied software patches, the firewalls left unattended, and the anti-virus suites that never get updated even in the U.S. military cause us more trouble than I like to admit, especially when a risk to one is a risk shared by all.

Therefore, the immediate notification of emerging vulnerabilities and timely resolution of those vulnerabilities is critical to the systems integrity.

Severity Categories

A Security Technical Implementation Guide Severity Category Code is a measure of risk to assess system security posture. For example, a Category I vulnerability allows unauthorized users to obtain immediate system access and represents the greatest security risk. In addition, a Category II vulnerability has the potential to lead to unauthorized system access.

---

[1] CYBERCOM is a sub-unified command that is subordinate to U.S. Strategic Command.

* See the Glossary, Appendix C, for definition.

DoD Information Assurance Vulnerability Alert Process

(~~FOUO~~) The DoD IAVM program includes the Information Assurance Vulnerability Alert (IAVA) process, which provides vulnerability notifications, corrective actions, and reporting requirements for DoD Components. Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 9, 2011, requires CYBERCOM to develop IAVAs based on their evaluation of vulnerabilities. CYBERCOM[2] representatives stated they analyze information assurance vulnerabilities received from Symantec Corporation and open sources and issue IAVAs for those vulnerabilities that present an immediate and severe threat to the DoD Global Information Grid.* For example, CYBERCOM issued IAVA 2011-A-0078 on June 16, 2011. This IAVA required DoD Components to either patch* vulnerable systems or have a plan of action and milestones (POA&M) with tasks and completion dates to mitigate or fix the vulnerability by July 7, 2011. According to the IAVA, this vulnerability could permit a denial of service attack* on the affected system.

(~~FOUO~~) Further, Chairman of the Joint Chiefs of Staff Instruction 6510.01F requires DoD Components, as directed by IAVAs, to take compliance actions and report compliance status. The IAVAs require DoD Components to either patch network devices, such as workstations or servers (assets), affected by a vulnerability described in an IAVA (affected assets) or prepare a POA&M for assets that they cannot patch. According to CYBERCOM representatives, the POA&M should outline the measures put in place to protect assets that they could not patch. In addition, the POA&M must be dated and approved by the designated approving authority. Preparing a POA&M for unpatched assets is critical because a POA&M creates a mechanism for ensuring that unpatched assets are brought to the attention of management and vulnerabilities are addressed in a timely manner. If vulnerabilities are not addressed in a timely manner, the DoD Component network and DoD Global Information Grid are at risk of loss, misuse, or unauthorized access to sensitive DoD information. CYBERCOM representatives stated that DoD Components report IAVA compliance in the DoD Vulnerability Management System (VMS). Then, CYBERCOM representatives used the VMS to track IAVA compliance.

DFAS

DFAS is a DoD Component established to provide finance and accounting services for DoD and other Federal activities. DFAS operates under the authority, direction, and control of the Comptroller of the DoD. DFAS representatives stated the DFAS unclassified network processed sensitive DoD information, such as financial information and personally identifiable information. The DFAS Chief Information Officer (CIO) is responsible for the DFAS IAVM program, including monitoring and reporting compliance.

---

[2] Before June 2010, the Joint Task Force-Global Network Operations issued the IAVAs. Beginning in June 2010, CYBERCOM began issuing the IAVAs.

* See the Glossary, Appendix C, for definition.

Review of Internal Controls

(~~FOUO~~) DoD Instruction 5010.40, "Managers' Internal Control Program (MICP) Procedures," July 29, 2010, requires DoD Components to establish a program to review, assess, and report on the effectiveness of their internal controls. We identified internal control weaknesses in the DFAS IAVM program. Specifically, DFAS did not have procedures that required them to report full compliance in VMS only when all affected assets were patched or procedures that required them to use current compliance reports and system administrators to identify affected assets for VMS reporting. We also identified other internal control weaknesses in DoD. Specifically, DoD did not update IAVM guidance on a timely basis and did not specify IAVA requirements for patching vulnerabilities identified after the POA&M mitigation date. In addition, DoD cancelled the IAVM program manual. Although we identified these internal control weaknesses, we did not make recommendations because Department of Defense Office of Inspector General (DoD OIG) Report No. D-2011-096, "Improvements Are Needed to the DoD Information Assurance Vulnerability Management Program," August 12, 2011, (DoD OIG Report D-2011-096), contained recommendations that should correct the internal control weaknesses. We will provide a copy of the report to the senior official responsible for internal controls at DoD CIO, DFAS, and the Joint Staff.

Finding. DFAS IAVA Remediation and Reporting Processes Need Improvement (~~FOUO~~)

(~~FOUO~~) The DFAS CIO did not always have effective processes in place to manage and mitigate system vulnerabilities. Specifically, as of October 2011, the DFAS CIO did not remediate[3] 507 of 1,007 Category I and II vulnerabilities identified on the DFAS network in August 2011. In addition, the DFAS CIO inaccurately reported full compliance in the VMS for 42 of 51 active Category I and II IAVAs between September 2010 and August 2011. Finally, the DFAS CIO could not support the number of affected assets reported in VMS for 28 of 52 sample IAVAs.

(~~FOUO~~) The processes that the DFAS CIO put in place were not always effective because they:

- permitted the use of a 99-percent asset compliance* threshold to mitigate vulnerabilities and
- did not mandate the use of compliance reports and system administrators to report affected assets in VMS.

(~~FOUO~~) Finally, this occurred because DoD issued inadequate IAVM program guidance. Specifically,

- DoD did not update the overarching IAVM guidance in more than 10 years;
- the Vice Director, Joint Staff cancelled the IAVM program manual; and
- the Chief of Dynamic Network Defense Operations for the CYBERCOM did not specify the IAVA requirements for patching vulnerabilities identified after the POA&M mitigation date.*

(~~FOUO~~) The combination of inadequate DFAS and DoD IAVM program guidance resulted in an increased risk of compromising sensitive DoD information, such as financial and personally identifiable information on the DFAS network. Given the vulnerabilities identified, an individual could gain unauthorized access to the DFAS network. Further, inaccurate IAVA compliance reporting in VMS by DoD Components can reduce the effectiveness of CYBERCOM IAVA compliance oversight, thereby increasing the risk that DoD Components will not remediate network vulnerabilities.

---

[3] Remediation consists of actions taken, such as patching or preparing a POA&M, to fix or otherwise mitigate a vulnerability on an affected asset.
* See the Glossary, Appendix C, for definition.

DFAS Did Not Always Effectively Manage and Mitigate System Vulnerabilities (~~FOUO~~)

(~~FOUO~~) The DFAS CIO did not always have effective processes in place to manage and mitigate system vulnerabilities. Specifically, the DFAS CIO did not remediate vulnerabilities, inaccurately reported compliance, and could not support VMS reporting.

DFAS Did Not Remediate Vulnerabilities (~~FOUO~~)

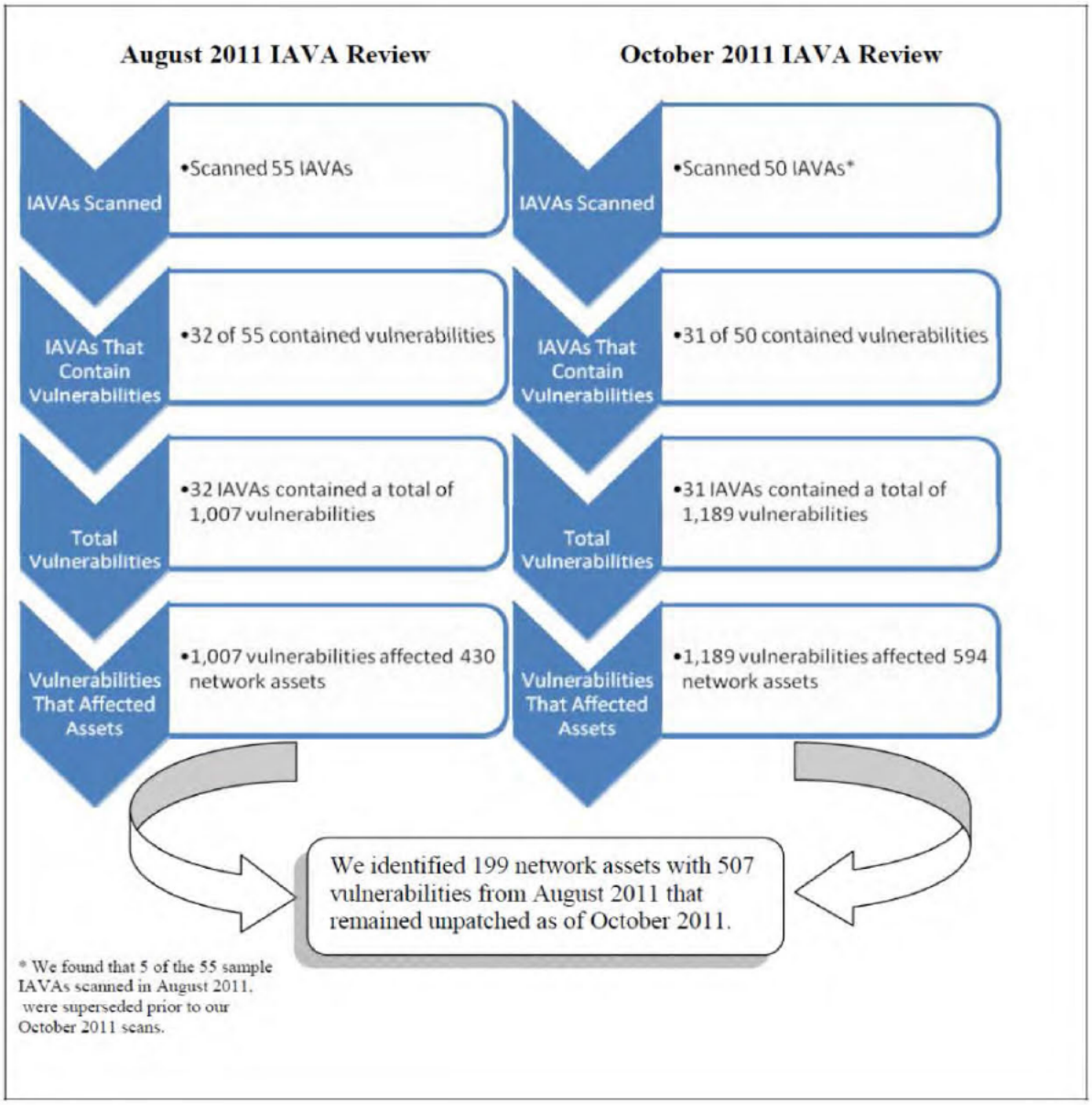
(~~FOUO~~) As of October 2011, the DFAS CIO did not remediate 507 of 1,007 Category I and II vulnerabilities identified on the DFAS network in August 2011. In August 2011 and October 2011, we asked DFAS to run vulnerability scans of the DFAS unclassified network to identify vulnerabilities associated with 55[4] and 50[5] sample IAVAs, respectively. To ensure proper configuration we observed DFAS personnel configure the vulnerability scans. The Joint Task Force-Global Network Operations and CYBERCOM[6] issued these IAVAs between January 2009 and June 2011 and classified the vulnerabilities in these IAVAs as either Category I or Category II. DFAS reported in VMS that all affected network assets were compliant for these IAVAs. However, based on the scan results, we identified 430 network assets with 1,007 vulnerabilities from 32 of 55 sample IAVAs in August 2011. In addition, we identified 594 network assets with 1,189 vulnerabilities from 31 of 50 sample IAVAs in October 2011. We identified 199 network assets with 507 vulnerabilities from August 2011 that remained unpatched as of October 2011.[7] In addition, DFAS did not place the 199 assets on a POA&M. According to CYBERCOM representatives, vulnerabilities identified after the POA&M mitigation date[8] should be immediately patched or immediately placed on a POA&M.

> ***(~~FOUO~~)*** *We identified 199 network assets with 507 vulnerabilities from August 2011 that remained unpatched as of October 2011.*

[4] **(~~FOUO~~)** When DFAS representatives scanned their network in August 2011, they scanned for 55 of 59 sample IAVAs because CYBERCOM superseded three IAVAs and we omitted one IAVA from the scan because of human error.
[5] **(~~FOUO~~)** By October 2011, CYBERCOM superseded an additional five sample IAVAs.
[6] Before June 2010, the Joint Task Force-Global Network Operations issued IAVAs. Beginning in June 2010, CYBERCOM began issuing IAVAs.
[7] **(~~FOUO~~)** In February 2012, DFAS representatives stated that 12 of 199 network assets with vulnerabilities from August 2011 that remained unpatched as of October 2011 were false positive assets. These 12 network assets included 19 of 507 vulnerabilities that remained unpatched. We did not determine whether the assets were false positive in August 2011 and October 2011.
[8] **(~~FOUO~~)** Each of the sample IAVAs had a POA&M mitigation date before July 15, 2011.

~~(FOUO)~~ The following figure provides a summary of the August 2011 and October 2011 scan results.

~~(FOUO)~~ Figure. Summary of Scan Results



DFAS Inaccurately Reported Compliance ~~(FOUO)~~

~~(FOUO)~~ The DFAS CIO inaccurately reported full compliance in the VMS for 42 of 51 active Category I and II IAVAs between September 2010 and August 2011. According to the August 2011 DFAS VMS compliance report, the DFAS CIO reported that all affected network assets were compliant; when in fact, not all affected network assets were compliant. DFAS representatives stated they used compliance reports as a source

~~(FOUO)~~ for reporting IAVA compliance in VMS. We reviewed DFAS compliance reports for 17 of 55 sample IAVAs. According to the compliance reports used to report in VMS, 14 of those IAVAs had noncompliant assets. For example, one of the 14 sample IAVAs was a February 2011 IAVA for which DFAS reported full compliance in VMS; however, the DFAS compliance report used to report in VMS showed this IAVA had 245 unpatched assets. In addition to 17 of 55 sample IAVAs, we also reviewed DFAS compliance reports used to report in VMS for 34 other IAVAs and identified 28 IAVAs with noncompliant assets. However, DFAS reported in VMS that these assets were fully compliant. By reporting full compliance, DFAS representatives avoided having to prepare POA&Ms for the noncompliant network assets.

DFAS Could Not Support VMS Reporting (~~FOUO~~)

~~(FOUO)~~ The DFAS CIO could not support the number of affected assets reported in VMS for 28 of 52 sample IAVAs. DFAS representatives stated that the number of assets on their network could change numerous times each day. However, the DFAS CIO reported constant numbers of affected assets in VMS. Specifically, according to the August 2011 DFAS VMS compliance report, between May 2010 and June 2011, the DFAS CIO reported DFAS: (b) (7)(E) affected assets for 16 of 52 sample IAVAs.[9] Further, between May 2009 and October 2010, the DFAS CIO reported DFAS: (b) (7)(E) affected assets for 12 of 52 sample IAVAs. DFAS representatives stated that they generally used compliance reports for workstations and correspondence from system administrators for nonworkstations to determine whether affected assets were patched; however, DFAS representatives did not always use these sources to identify the number of affected assets reported in VMS. Instead, DFAS representatives said they performed periodic network queries to identify the total number of DFAS network assets and then reported that number in VMS, for an extended period of time, as affected assets. As a result, the number of affected assets reported by DFAS in VMS may differ from the number of affected assets that could be obtained from compliance reports and system administrators.

DFAS Did Not Have Adequate Internal Guidance (~~FOUO~~)

~~(FOUO)~~ The DFAS CIO did not remediate vulnerabilities, report accurate compliance, and could not support VMS reporting because DFAS had inadequate internal guidance. Specifically, DFAS permitted the use of a 99-percent asset compliance threshold and DFAS did not mandate use of compliance reports and system administrators for reporting affected assets in VMS.

DFAS Permitted 99-Percent Compliance Threshold (~~FOUO~~)

~~(FOUO)~~ The DFAS CIO permitted the use of a 99-percent asset compliance threshold to mitigate vulnerabilities.[10] This permitted DFAS representatives to report in VMS that all affected network assets were patched if DFAS patched 99 percent of the affected network

---

[9] **~~(FOUO)~~** By August 2011, CYBERCOM superseded 5 of 59 sample IAVAs. In addition, DFAS representatives reported in their August 2011 VMS compliance report that 2 other sample IAVAs were not applicable to DFAS leaving 52 of 59 sample IAVAs for our review.

[10] **~~(FOUO)~~** As of August 2011, DFAS reported approximately 15,000 assets in VMS.

~~(FOUO)~~ assets. Further, DFAS did not have to issue POA&Ms for the remaining 1 percent of noncompliant assets. Specifically, DFAS representatives could report that all assets were patched, but still have up to 150 assets unpatched. Further, by reporting that all affected network assets are patched, DFAS would not have to place the noncompliant assets on a POA&M. DoD IAVAs state that compliance with the IAVA is mandatory and require DoD Components to have an approved POA&M in place by the POA&M mitigation date for vulnerabilities that cannot be patched within the required timeline. However, according to the DFAS Initial Notice Procedure guidance, once an IAVA reaches 99-percent asset compliance, DFAS representatives would move the VMS numbers to 100 percent compliance. In addition, according to DFAS representatives, they did not prepare a POA&M if they were able to patch at least 99 percent of the affected assets for an IAVA. Consequently, DFAS officials might not have patched 1 percent of their assets affected by an IAVA or placed those assets on a POA&M by the POA&M mitigation date. If DFAS does not address all vulnerabilities in a timely manner, its network and the DoD Global Information Grid are at risk of loss, misuse, or unauthorized access to sensitive DoD Information.

> ***~~(FOUO)~~*** *Specifically, DFAS could report that all assets were patched, but still have up to 150 assets unpatched.*

~~(FOUO)~~ CYBERCOM representatives stated the 99-percent asset compliance threshold for reporting IAVM compliance was inappropriate and did not provide a true risk assessment to the DoD Global Information Grid. DFAS should report full IAVA compliance in the VMS only when all affected network assets are patched. In addition, DFAS should revise internal guidance to require DFAS to report full IAVA compliance in VMS only when all affected network assets are patched. Finally, the DFAS Deputy Director, Strategy and Support should review the actions of the DFAS CIO to determine if he acted within the scope of his authority to use a 99-percent asset compliance threshold to mitigate vulnerabilities and take appropriate actions. In December 2011, DFAS representatives stated they would ensure that all vulnerabilities are 100 percent compliant when reporting compliance in VMS. This would be a positive step by DFAS.

~~(FOUO)~~ Further, the DFAS CIO did not always properly approve POA&Ms by the POA&M mitigation date, which varies based on the IAVA. CYBERCOM representatives stated the designated approving authority should approve POA&Ms by the POA&M mitigation date. We reviewed the August 2011 DFAS VMS compliance report for 52 sample IAVAs. According to this report, DFAS reported in VMS that assets associated with 18 of 52 sample IAVAs were on a POA&M as of the POA&M mitigation date. However, DFAS representatives provided POA&Ms for only 11 IAVAs and the DFAS CIO[11] did not approve any by the POA&M mitigation date. For example, the DFAS CIO approved one POA&M 25 days after the POA&M mitigation date. DFAS did not provide POA&Ms for the remaining seven IAVAs. For example, according to DFAS representatives, they did not prepare a POA&M for two of these seven IAVAs

[11] According to DFAS representatives, the DFAS CIO is also the DFAS designated approving authority.

~~(FOUO)~~ because they deployed the patches, but reported 1 day late.[12] The DFAS CIO should approve a POA&M for all DFAS affected network assets that are not patched by the POA&M mitigation date in the corresponding IAVA. In December 2011, DFAS representatives stated they would ensure the DFAS CIO receives the POA&M package in sufficient time to obtain signature by the POA&M mitigation date. This would be a positive step by DFAS.

DFAS Did Not Mandate Use of Compliance Reports and System Administrators for VMS Reporting (~~FOUO~~)

~~(FOUO)~~ In addition, the DFAS CIO did not mandate the use of compliance reports and system administrators to report affected assets in VMS. Specifically, according to the DFAS IAVM Initial Notice Procedure guidance, DFAS representatives may obtain affected asset numbers from weekly compliance reports and/or system managers[13] for reporting in VMS. However, the guidance does not clearly mandate that DFAS representatives must obtain affected asset numbers from compliance reports and/or system administrators for reporting in VMS. Consequently, the number of affected assets DFAS reported in VMS was most likely inaccurate, providing CYBERCOM invalid information. Since DFAS representatives said they used compliance reports and correspondence from system administrators to determine whether DFAS was compliant with an IAVA, DFAS should be consistent and also use compliance reports and system administrators to identify the number of affected assets to report in VMS. In addition, DFAS should revise internal guidance to clearly mandate use of compliance reports and system administrators to identify the number of affected assets to report in VMS. In December 2011, DFAS representatives said they would use compliance reports and responses from system administrators in determining affected assets and compliance. This would be a positive step by DFAS.

DoD Did Not Have Adequate IAVM Program Guidance

~~(FOUO)~~ Also, the DFAS CIO did not remediate vulnerabilities, report accurate compliance, and could not support VMS reporting because DoD issued inadequate IAVM program guidance. Specifically, DoD did not update overarching IAVM guidance, cancelled the IAVM program manual, and did not specify the IAVA requirements for patching vulnerabilities identified after the POA&M mitigation date.

Overarching IAVM Guidance Needs Updating

DoD did not update the overarching IAVM guidance in more than 10 years. DoD Instruction 5025.01, "DoD Directives Program," October 28, 2007, requires all DoD directives and instructions to be reviewed before the 5-year anniversary of their publication date to ensure they are necessary, current, and consistent with DoD policy, existing law, and statutory authority. The directives and instructions should then be

---

[12] **~~(FOUO)~~** Four of the remaining IAVAs were from 2009 when, according to DFAS representatives, DFAS did not have a centralized POA&M filing system. DFAS did not provide the remaining POA&M.
[13] According to DFAS representatives, this should be system administrators instead of system managers.

reissued, certified as current, or cancelled as a result of the review. All directives and instructions certified as current should either be revised and reissued or cancelled within 7 years of their publication dates.

~~(FOUO)~~ DoD Directive O-8530.1, "Computer Network Defense," January 8, 2001, and DoD Instruction O-8530.2, "Support to Computer Network Defense (CND)," March 9, 2001, provide overarching guidance for the DoD IAVA process to include IAVA issuance, compliance reporting, and monitoring. However, these documents have not been reissued, certified as current, or cancelled since their publication dates in 2001.[14] Therefore, there was no assurance that the IAVA guidance in the directive and instruction are "necessary, current, and consistent with DoD policy, existing law, and statutory authority." In DoD OIG Report D-2011-096, we recommended the Assistant Secretary of Defense (Networks and Information Integration)/DoD CIO establish milestones and update DoD Directive O-8530.1 and DoD Instruction O-8530.2. The DoD CIO agreed and stated DoD Directive O-8530.1 and DoD Instruction O-8530.2 were being updated. Followup actions for this recommendation are pending. Since we made this recommendation in DoD OIG Report D-2011-096, we did not make the recommendation again.

IAVM Program Manual Needs to Be Updated

In June 2009, the Vice Director, Joint Staff cancelled the manual that provided responsibilities and procedures for the DoD IAVM program.[15] The manual required DoD Components to report compliance status in the VMS for all IAVAs, including the number of assets affected, compliant, and on a POA&M. In DoD OIG Report D-2011-096, we recommended the Joint Staff establish milestones and update the DoD IAVM program manual. The Joint Staff representative agreed and stated that the Joint Staff is assisting CYBERCOM in updating the vulnerability management program guidance to be published in a Chairman of the Joint Chiefs of Staff manual within the agreed set of milestones. Followup actions for this recommendation are pending. Since we made this recommendation in DoD OIG Report D-2011-096, we did not make the recommendation again.

Remediation Guidance for Vulnerabilities Identified After the POA&M Mitigation Date

~~(FOUO)~~ The Chief of Dynamic Network Defense Operations for the CYBERCOM did not specify the IAVA requirements for patching vulnerabilities identified after the

---

[14] **~~(FOUO)~~** When DoD issued Directive O-8530.1 and Instruction O-8530.2 in 2001, the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence was responsible for computer network defense policy direction and guidance. In 2005, DoD established the Assistant Secretary of Defense for Networks and Information Integration/DoD CIO, which was the office primarily responsible for DoD Directive O-8530.1 and DoD Instruction O-8530.2. As of January 11, 2012, the DoD CIO is the primary DoD authority for computer network defense policy.

[15] The cancelled manual was the Chairman of the Joint Chiefs of Staff Manual 6510.01 Change 2, Appendix A to Enclosure B, "Information Assurance Vulnerability Management Program," January 26, 2006.

~~(FOUO)~~ POA&M mitigation date. Specifically, Joint Task Force-Global Network Operations issued 33 of 55 sample IAVAs we reviewed and CYBERCOM issued the remaining 22 of 55 sample IAVAs we reviewed.[16] Those IAVAs provide a POA&M mitigation date, by which DoD Components must either patch vulnerabilities or have a POA&M in place. However, the IAVAs did not specify a timeline for patching or reporting vulnerabilities identified after the POA&M mitigation date. In DoD OIG Report D-2011-096, we recommended that CYBERCOM officials revise DoD IAVAs to provide a remediation timeline by which DoD Components should either patch or prepare a POA&M for vulnerabilities identified after the POA&M mitigation date. In December 2011 CYBERCOM revised DoD IAVAs to provide a remediation timeline by which DoD Components should either patch or prepare a POA&M for vulnerabilities identified after the POA&M mitigation date.

DFAS Increased Risk of Compromising Sensitive Information on Its Network ~~(FOUO)~~

~~(FOUO)~~ The combination of DFAS permitting the use of a 99-percent asset compliance threshold, DFAS not mandating the use of compliance reports and system administrators to report in VMS, and DoD issuing inadequate IAVM program guidance resulted in an increased risk of compromising sensitive DoD information, such as financial and personally identifiable information on the DFAS network. According to DFAS representatives, DFAS had technical controls including Intrusion Detection and Prevention Systems, firewalls with access control lists, host security deployed to each DFAS asset, current Host Intrusion Prevention Sensors, and a Security Information Events Management Solution. According to DFAS representatives, reporting full IAVA compliance while not remediating up to 1 percent of vulnerabilities would result in minimal risk because of their technical controls. According to CYBERCOM representatives, patching network assets that have vulnerabilities identified in an IAVA is the first line of defense to protect those assets. Other controls, such as intrusion detection systems and firewalls, can help to mitigate the effects of vulnerable assets but all of the network controls that are in place work together to provide a layered defense and reduce the security risk for the network. If a Component removes one of the controls, especially patching[17], they increase the risk of compromise to that network from vulnerable assets. We were not made aware of any network breaches. However, successful exploitation of vulnerabilities identified would result in an adversary gaining unauthorized access to the DFAS network. In addition, the adversary could deny authorized users access to the DFAS network. Further, inaccurate IAVA compliance

> ***~~(FOUO)~~*** *However, successful exploitation of vulnerabilities identified would result in an adversary gaining unauthorized access to the DFAS network.*

[16] Before June 2010, the Joint Task Force-Global Network Operations issued IAVAs. Beginning in June 2010, CYBERCOM began issuing IAVAs.

[17] According to CYBERCOM representatives, for vulnerabilities identified in an IAVA, the security risk to a Component network with vulnerable assets is less if the Component patches those assets than if the Component relies on other mitigating controls to protect the vulnerable assets on the network.

~~(FOUO)~~ reporting in VMS by DoD Components can reduce the effectiveness of CYBERCOM IAVA compliance oversight, thereby increasing the risk that DoD Components will not remediate network vulnerabilities. Specifically, if a DoD Component inaccurately reports affected assets as fully compliant in VMS, CYBERCOM cannot use VMS to readily identify those vulnerable assets for followup action. Therefore, DFAS needs to initiate action to strengthen their IAVM program.

Recommendations, Management Comments, and Our Response

Redirected Recommendation

As a result of management comments, we redirected draft report Recommendation 2 to the DFAS Deputy Director, Strategy and Support. However, no additional comments are required as the response provided by the Deputy Director to the draft of this report met the intent of the recommendation.

1. We recommend that the Chief Information Officer, Defense Finance and Accounting Service:

a. ~~(FOUO)~~ Report full Information Assurance Vulnerability Alert compliance in the Vulnerability Management System only when all affected network assets at Defense Finance and Accounting Service are patched.

DFAS Comments

~~(FOUO)~~ Responding for the DFAS CIO, the DFAS Deputy Director, Strategy and Support (hereafter referred to as the Deputy Director), agreed and stated that DFAS processes and procedures were changed in December 2011 with documentation completed in January 2012. The Deputy Director also stated that the current DFAS process requires 100-percent compliance to report IAVA closure. Finally, the Deputy Director stated that devices identified in scans are patched immediately or tracked and managed with POA&Ms for each scan result.

Our Response

The comments from the Deputy Director were responsive, and no further comments are required.

b. ~~(FOUO)~~ Revise internal guidance to require Defense Finance and Accounting Service to report full Information Assurance Vulnerability Alert compliance in the Vulnerability Management System only when all affected network assets are patched.

DFAS Comments

~~(FOUO)~~ The Deputy Director agreed and stated that DFAS processes and procedures were changed in December 2011 with documentation completed in January 2012. The Deputy Director also stated that the current DFAS process requires 100-percent compliance to report IAVA closure. Finally, the Deputy Director stated that devices identified in scans are patched immediately or tracked and managed with POA&Ms for each scan result.

Our Response

The comments from the Deputy Director were responsive, and no further comments are required.

c. ~~(FOUO)~~ Approve a plan of action and milestones for all affected network assets at Defense Finance and Accounting Service that are not patched by the plan of action and milestones mitigation date in the corresponding Information Assurance Vulnerability Alert.

DFAS Comments

~~(FOUO)~~ The Deputy Director agreed and stated that updated procedures require that the DFAS CIO receive the POA&M to approve before the POA&M mitigation date.

Our Response

~~(FOUO)~~ The comments from the Deputy Director were partially responsive. Although the Deputy Director states that updated procedures require that the DFAS CIO receive the POA&M to approve before the POA&M mitigation date, neither the comments nor updated procedures provided by DFAS clearly state that the DFAS CIO would approve POA&Ms by the POA&M mitigation date. As a result, we request that the DFAS CIO provide additional comments in response to the final report to clarify whether the DFAS CIO will approve POA&Ms by the POA&M mitigation date and to ensure that procedures are updated to reflect this requirement.

d. ~~(FOUO)~~ Use compliance reports and system administrators to identify the number of affected assets to report in the Vulnerability Management System.

DFAS Comments

~~(FOUO)~~ The Deputy Director agreed and stated that DFAS processes and procedures were changed in December 2011 with documentation updated in January 2012. The Deputy Director also stated that DFAS has been using compliance reports and system administrators to identify the number of affected assets to report in VMS.

Our Response

The comments from the Deputy Director were responsive, and no further comments are required.

e. ~~(FOUO)~~ Revise internal guidance to mandate that Defense Finance and Accounting Service use compliance reports and system administrators to identify the number of affected assets to report in the Vulnerability Management System.

DFAS Comments

~~(FOUO)~~ The Deputy Director agreed and stated that DFAS processes and procedures were changed in December 2011 with documentation updated in January 2012. The Deputy Director also stated that DFAS has been using compliance reports and system administrators to identify the number of affected assets to report in VMS.

Our Response

~~(FOUO)~~ The comments from the Deputy Director were partially responsive. The Deputy Director stated that DFAS processes and procedures were changed and DFAS has been using compliance reports and system administrators to identify affected assets to report in VMS. However, updated procedures provided by DFAS do not mandate that DFAS use compliance reports and system administrators to identify the number of affected assets to report in VMS. As a result, we request that the DFAS CIO provide additional comments in response to the final report.

2. ~~(FOUO)~~ We recommend that the Defense Finance and Accounting Service Deputy Director, Strategy and Support review the actions of the Defense Finance and Accounting Service Chief Information Officer to determine if he acted within the scope of his authority to use a 99-percent asset compliance threshold to mitigate vulnerabilities and take appropriate actions.

DFAS Comments

~~(FOUO)~~ Responding for the Director, DFAS, the Deputy Director, Strategy and Support (hereafter referred to as the Deputy Director) stated this finding, which was directed to the Director, DFAS in the draft report, should be directed to the Deputy Director to whom the DFAS CIO reports. Otherwise, the Deputy Director agreed and stated that the DFAS CIO is the Designated Accrediting Authority for DFAS and CYBERCOM requires Designated Accrediting Authority approval and reporting in VMS for POA&Ms associated with IAVAs. However, the Deputy Director stated that use of the 99-percent threshold was done by a subordinate, without DFAS CIO knowledge or consent. The Deputy Director also stated that the subordinate did not have authority to use the lower threshold. Further, the Deputy Director stated that the CIO took action to correct the act of the subordinate and ensure that similar actions would not occur in the future. Finally, the Deputy Director stated that the current process requires 100-percent compliance to report IAVA closure.

Our Response

The comments from the Deputy Director were responsive, and no further comments are required. As a result of the Deputy Director comments, we redirected draft report Recommendation 2 to the Deputy Director, Strategy and Support.

Appendix A. Scope and Methodology

We conducted this performance audit from June 2011 through March 2012 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

~~(FOUO)~~ We selected DFAS because they possessed a large number of assets and were self-reporting 100-percent compliance for most of their IAVAs in the VMS.

~~(FOUO)~~ We interviewed representatives from DFAS to identify their practices pertaining to the DoD IAVM program. We also coordinated with representatives from U.S. Strategic Command, CYBERCOM, Assistant Secretary of Defense for Networks and Information Integration/DoD CIO,[18] Defense Information Systems Agency, and the Joint Staff. In addition, we reviewed criteria governing the IAVM program, such as DoD Instruction O-8530.2, "Support to Computer Network Defense (CND)," March 9, 2001; DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003; and Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 9, 2011. We also reviewed the DFAS internal guidance on their IAVM program.

~~(FOUO)~~ We selected 59 IAVAs issued between January 2009 and June 2011. We selected 39 Category I IAVAs because of the high risk associated with Category I vulnerabilities. We also selected 20 Category II IAVAs for review. Our sampling methodology is provided in Appendix B.

We performed site visits to DFAS Indianapolis, Indiana, from August 15, 2011, through August 19, 2011, and from October 24, 2011 through October 27, 2011. During our site visits in August 2011 and October 2011, we asked DFAS personnel to scan the DFAS network for vulnerabilities associated with our sample, and we observed these scans. To ensure proper configuration, we observed DFAS personnel configure the vulnerability scans. The DoD OIG Information Systems Directorate provided assistance before our first DFAS site visit in August 2011. Specifically, an Information Systems Directorate representative gave the audit team an overview of scan configurations to help the team ensure DFAS properly configured the tool.

[18] As of January 11, 2012, the Deputy Secretary of Defense disestablished the position of Assistant Secretary of Defense for Networks and Information Integration/DoD CIO and transferred those authorities, responsibilities, personnel, and resources to the DoD CIO.

~~(FOUO)~~ We then compared the two site visit scan results to determine whether DFAS patched their affected network assets in a timely manner. We also reviewed DFAS POA&Ms to determine whether DFAS had properly and timely remediated affected network assets. Finally, we reviewed DFAS internal correspondence for 51 IAVAs reported as fully compliant between September 2010 and August 2011 in VMS to assess the accuracy of DFAS reporting in VMS.

Use of Computer-Processed Data

We used computer-processed data from the Retina scans performed on DFAS's unclassified network. Retina is the DoD-recommended Secure Configuration Compliance Validation Initiative tool. We obtained reasonable assurance of the reliability of data resulting from the Retina scan by ensuring the tool was appropriately configured to complete a proper scan. Specifically, we observed DFAS personnel configure the vulnerability scans. In addition, a DoD OIG Network Compliance Engineer gave the audit team an overview of scan configurations before the first site visit. On the basis of this work, we concluded that the data were sufficiently reliable for the purpose of our review.

Use of Technical Assistance

The DoD OIG Quantitative Methods Division assisted with the audit. See Appendix B for detailed information about the work performed by the Quantitative Methods Division.

Prior Coverage

During the last 5 years, the DoD OIG issued one report on the DoD IAVM program.

DoD OIG

DoD OIG Report No. D-2011-096, "Improvements Are Needed to the DoD Information Assurance Vulnerability Management Program," August 12, 2011

Appendix B. Sampling Methodology

Population

~~(FOUO)~~ The population consisted of 107 IAVAs issued between January 2009 and June 2011 and included 39 Category I IAVAs and 68 Category II IAVAs. There were no dollar values associated with the IAVAs. We selected all Category I IAVAs because of the high risk associated with Category I vulnerabilities. The DoD OIG Quantitative Methods Division selected Category II IAVAs using a simple random selection. See the following table for the population and sample sizes.

~~(FOUO)~~ Table. Population and Sample Sizes

IAVA Category	Population Size	Sample Size
I	39	39
II	68	20

Results

~~(FOUO)~~ The Category II IAVA population changed over time so DoD OIG Quantitative Methods Division did not project the Category II IAVA sample. As a result, only the sample results were reported.

Appendix C. Glossary

For purposes of this report, we defined specific technical terms as follows:

Compliant Asset - An asset that is affected by an IAVA but has a permanent fix to address the vulnerability described in that IAVA.

Denial of Service Attack - Deliberate actions taken to circumvent information system security and prevent authorized access to system resources or delay time-critical operations.

Global Information Grid - The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel.

Patch - Implementation of a solution prescribed by an IAVA to permanently fix a vulnerability described in that IAVA.

POA&M Mitigation Date - The date provided in an IAVA by which all affected assets must either be patched or put on an approved POA&M.

Remediation - Actions taken, such as patching or preparing a POA&M, to fix or otherwise mitigate a vulnerability on an affected asset.

Vulnerability - An information system security weakness that could be exercised to gain unauthorized access to an information system.

Defense Finance and Accounting Service Comments

~~FOR OFFICIAL USE ONLY~~

DEFENSE FINANCE AND ACCOUNTING SERVICE
P.O. BOX 182317
Columbus, OH 43218-2317

DFAS-Z

MEMORANDUM FOR (b) (6) PROGRAM DIRECTOR, READINESS, OPERATIONS, AND SUPPORT, OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: Response to Draft Report (Project No. D2011-D000LB-0230.000)

On behalf of the DFAS Director, this memorandum responds to Draft Report, Improvements are Needed to the Defense Finance and Accounting Service Information Assurance Vulnerability Management Program, (Project No. D2011-D000LB-0230.000), dated March 14, 2012.

Recommendations, Page 12, Item 1. We recommend that the Chief Information Officer, Defense Finance and Accounting Service:

a. Report full Information Assurance Vulnerability Alert compliance in the Vulnerability Management System only when all affected network assets at Defense Finance and Accounting Service are patched.

Response: Concur. DFAS processes and procedures were changed December 21, 2011 with documentation completed January 12, 2012. Our current process requires 100% compliance to report IAVA closure. Devices identified in scans are patched immediately or tracked and managed with POA&Ms for each scan result. We consider this item closed.

b. Revise internal guidance to require Defense Finance and Accounting Service to report full Information Assurance Vulnerability Alert compliance in the Vulnerability Management System only when all affected network assets are patched.

Response: Concur. DFAS processes and procedures were changed December 21, 2011 with documentation completed January 12, 2012. Our current process requires 100% compliance to report IAVA closure. Devices identified in scans are patched immediately or tracked and managed with POA&Ms for each scan result. We consider this item closed.

c. Approve a plan of action and milestones for all affected network assets at Defense Finance and Accounting Service that are not patched by the plan of action and milestones mitigation date in the corresponding Information and Assurance Vulnerability Alert.

Response: Concur. Updated procedures require that the DFAS CIO receive the POA&M to approve prior to the POA&M mitigation date. We consider this item closed.

d. Use compliance reports and system administrators to identify the number of affected assets to report in the Vulnerability Management System.

www.dfas.mil
Your Financial Partner @ Work

~~FOR OFFICIAL USE ONLY~~

Final Report Reference

~~FOR OFFICIAL USE ONLY~~

Response: Concur. DFAS processes and procedures were changed December 21, 2011 with documentation updated January 12, 2012. DFAS has been using compliance reports and system administrators to identify the number of affected assets to report in Vulnerability Management System. We consider this item closed.

e. Revise internal guidance to mandate that Defense Finance and Accounting Service use compliance reports and system administrators to identify the number of affected assets to report in the Vulnerability Management System.

Response: Concur. DFAS processes and procedures were changed December 21, 2011 with documentation updated January 12, 2012. DFAS has been using compliance reports and system administrators to identify the number of affected assets to report in Vulnerability Management System. We consider this item closed.

Recommendations, Page 12, Item 2. We recommend that the Director, Defense Finance and Accounting Service, review the actions of the Defense Finance and Accounting Service Chief Information Officer to determine if he acted within the scope of his authority to use a 99-percent asset compliance threshold to mitigate vulnerabilities and take appropriate actions.

Redirected, Page 14

Response: Concur. This finding should be directed to the DFAS Deputy Director, Strategy and Support, to whom the DFAS CIO reports. Regarding the question of authority, in accordance with DFAS 8500.1-R, the CIO is the Designated Accrediting Authority (DAA) for DFAS. The United States Cyber Command (USCYBERCOM) requires DAA approval and reporting in the Vulnerability Management System (VMS) for POA&M associated with Information Assurance Vulnerability Alerts (IAVAs). The use of a 99% threshold was done by a subordinate without the CIO's knowledge or consent. The subordinate did not have the authority to use the lower threshold. The CIO has taken action to correct the ultra vires act of the subordinate as well as to ensure that the similar actions would not occur in the future. The current process requires 100% compliance to report IAVA closure. We consider this item closed.

While the findings in this report do not identify any specific vulnerability that an outside entity could exploit, DFAS feels that release of this report may increase the number of attempts against the DFAS network. DFAS requests that the report be withheld from public release.

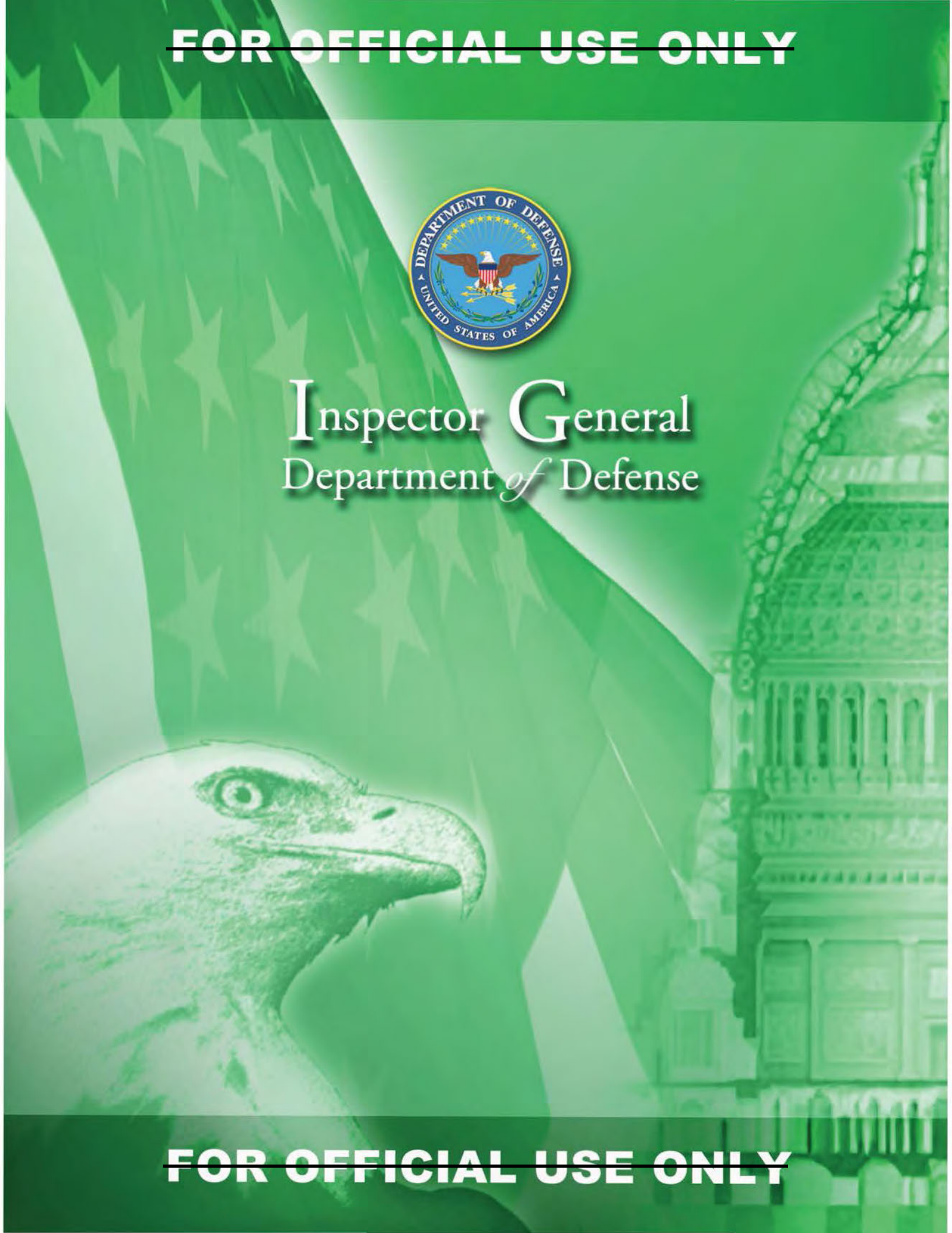
(b) (6) [redacted]

you for your assistance.

(b) (6) [redacted]

Jonathan Witter
Deputy Director, Strategy and Support

~~FOR OFFICIAL USE ONLY~~



FOR OFFICIAL USE ONLY